Security #7267 CLOSED

ja4: non alphanumeric characters in alpn lead to panic

Added by Philippe Antoine over 1 year ago. Updated over 1 year ago.

Status:	Closed		
Priority:	Normal		
Assignee:	Philippe Antoine		
Target version:	8.0.0-beta1		
Affected Versions:		**Git IDs:**	1e152d1f1060a5afd39496d4f2556e7159cd22cc
Label:			
CVE:	2024-47522	**Severity:**	CRITICAL
		Disclosure Date:	12/23/2024

Description

Found by oss-fuzz:
https://issues.oss-fuzz.com/issues/368729563

And we did not follow what the spec described for the case https://github.com/FoxIO-LLC/ja4/blob/main/technical_details/JA4.md#alpn-extension-value

Subtasks 1 (0 open — 1 closed)

~~Security #7268~~: ja4: non alphanumeric characters in alpn lead to panic (7.0.x backport)	Closed	Philippe Antoine

History | Notes | Property changes

Updated by OISF Ticketbot over 1 year ago #1

- **Subtask** *#7268* added

Updated by OISF Ticketbot over 1 year ago #2

- **Label** deleted (~~*Needs backport to 7.0*~~)

Updated by Philippe Antoine over 1 year ago #3

- **Status** changed from *New* to *In Review*
- **Label** *Needs backport to 7.0* added

Gitlab MR

Updated by Philippe Antoine over 1 year ago #4

- **Label** deleted (~~*Needs backport to 7.0*~~)

Updated by Philippe Antoine over 1 year ago #5

Stack trace :

```
thread '<unnamed>' panicked at src/ja4.rs:265:16:
source slice length (37) does not match destination slice length (36)

    #0 0x7adeac77f00b in raise /build/glibc-LcI20x/glibc-2.31/sysdeps/unix/sysv/linux/raise.c:51:1
    #1 0x7adeac75e858 in abort /build/glibc-LcI20x/glibc-2.31/stdlib/abort.c:79:7
    #2 0x5a3fa7ac8086 in std::sys::pal::unix::abort_internal::h6262fe410407344a /rustc/1a648b397dedc
    #3 0x5a3fa7abdab8 in rust_panic /rustc/1a648b397dedc98ada3dd3360f6d661ec2436c56/library/std/src/
    #4 0x5a3fa7abd899 in std::panicking::rust_panic_with_hook::haac9f65a4111ce33 /rustc/1a648b397dec
    #5 0x5a3fa7abd5a1 in std::panicking::begin_panic_handler::_$u7b$$u7b$closure$u7d$$u7d$::h6a452ac
    #6 0x5a3fa7abaaa5 in std::sys_common::backtrace::__rust_end_short_backtrace::ha4c176c669fc3286 /
    #7 0x5a3fa7abd2f3 in rust_begin_unwind /rustc/1a648b397dedc98ada3dd3360f6d661ec2436c56/library/s
    #8 0x5a3fa49e5fd4 in core::panicking::panic_fmt::hfae197985af26789 /rustc/1a648b397dedc98ada3dd3
    #9 0x5a3fa49e66f1 in core::slice::_$LT$impl$u20$$u5b$T$u5d$$GT$::copy_from_slice::len_mismatch_f
    #10 0x5a3fa5799db2 in core::slice::_$LT$impl$u20$$u5b$T$u5d$$GT$::copy_from_slice::h18261594c9e1
    #11 0x5a3fa5799db2 in SCJA4GetHash suricata/rust/src/ja4.rs:265:5
    #12 0x5a3fa4bcdb3c in GetData suricata/src/detect-ja4-hash.c:147:9
    #13 0x5a3fa4b5efb3 in PrefilterMpm suricata/src/detect-engine-prefilter.c:727:32
    #14 0x5a3fa4b58c9a in DetectRunPrefilterTx suricata/src/detect-engine-prefilter.c:125:9
    #15 0x5a3fa4ff0818 in DetectRunTx suricata/src/detect.c:1466:13
    #16 0x5a3fa4ff0818 in DetectRun suricata/src/detect.c:174:9
    #17 0x5a3fa4febb78 in Detect suricata/src/detect.c:0
    #18 0x5a3fa4c73ff5 in FlowWorker suricata/src/flow-worker.c:636:9
    #19 0x5a3fa4ac19d9 in LLVMFuzzerTestOneInput suricata/src/tests/fuzz/fuzz_sigpcap_aware.c:179:13
```

VJ Updated by Victor Julien over 1 year ago #6

- **Severity** changed from *MODERATE* to *CRITICAL*

JF Updated by Juliana Fajardini Reichow over 1 year ago #7

- **CVE** set to *2024-47522*

https://github.com/OISF/suricata/security/advisories/GHSA-w5xv-6586-jpm7

PA Updated by Philippe Antoine over 1 year ago #8

- **Status** changed from *In Review* to *Closed*

https://github.com/OISF/suricata/commit/1e152d1f1060a5afd39496d4f2556e7159cd22cc

PA Updated by Philippe Antoine over 1 year ago #9

- **Git IDs** updated (diff)

VJ Updated by Victor Julien over 1 year ago #10

- **Private** changed from *Yes* to *No*